M. ANDERSON BERRY (*pro hac vice* forthcoming)
GREGORY HAROUTUNIAN (*pro hac vice* forthcoming)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Facsimile: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com

BETSY C. MANIFOLD (*pro hac vice* forthcoming)
RACHELE R. BYRD (*pro hac vice* forthcoming)
OANA CONSTANTIN (*pro hac vice* forthcoming)
WOLF HALDENSTEIN ADLER
FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: (619) 239-4599
Facsimile: (619) 234-4599
manifold@whafh.com
byrd@whafh.com
constantin@whafh.com

Attorneys for Plaintiff and the Proposed Class

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

DAVID BAROCAS, individually and on behalf of all others similarly situated,

Plaintiff,

v.

TTEC SERVICES CORPORATION,

Defendant.

Case No.: _____

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff David Barocas ("Plaintiff"), in his individual capacity and on behalf of all others similarly situated, brings this Class Action Complaint against TTEC Services Corporation ("Defendant" or "TTEC") and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard Personally Identifiable Information ("PII") of its customers and employees, including, without limitation, their names, dates of birth, Healthcare ID number, medical record information, including clinical information such as diagnosis, and/or Social Security numbers.

2. Plaintiff also alleges Defendant failed to provide timely, accurate, and adequate notice to Plaintiff and similarly situated current and former employees and customers ("Class Members") that their PII had been lost and precisely what type of information was unencrypted and is now in the possession of unknown third parties.

3. Defendant is a customer experience and technology company that operates nationwide, offering its services to business clients. Defendant's employees and customers entrust it with an extensive amount of their PII. Defendant retains this information—even after the employment and customer relationships end.

4. On or around September of 2021, Defendant learned "there was unauthorized activity in [TTEC's] network between March 31, 2021 and September 12, 2021."[1] A hacker gained access to directories where PII was stored and obtained files stored on some of TTEC's servers (the "Data Breach"). TTEC completed a review of those files and other files on the servers on November 24, 2021, and determined that one or more of the files contained customers' and employees' names and Social Security numbers.[2]

5. In December, three months later, Defendant issued notice letters to those whose PII

---

[1] *See* **Exhibit A** attached hereto (letter from TTEC to Plaintiff Barocas dated December 8, 2021).

[2] *See* **Exhibit A**; https://oag.ca.gov/system/files/Health%20Net%20-%20TTEC%20Notification%20Letter.pdf (last visited Feb. 8, 2022); https://apps.web.maine.gov/online/aeviewer/ME/40/a49c129b-d8d5-4f09-beae-9135d8726541.shtml (with link to "Copy of notice to affected Maine residents: TTEC-ME App & Sample.pdf" last visited Feb. 8, 2022).

may have been impacted.

6. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant admits that the unencrypted PII that the attacker viewed and took included individuals' names, date of birth, Healthcare ID number, medical record information, including clinical information such as diagnosis, and/or Social Security numbers.[3]

7. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. The exposed PII of Plaintiff and Class Members can be sold on the dark web. Plaintiff and Class Members now face a present and lifetime risk of identity theft, which is heightened here by the loss of Social Security and date of birth information.

8. This PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiff and Class Members. In addition to Defendant's failure to prevent the Data Breach, after discovering the breach, Defendant waited three months to report it to the states' Attorneys General and affected individuals. Defendant has not informed Plaintiff or Class Members what the specific vulnerabilities and root causes of the breach were.

9. As a result of this delayed response, Plaintiff and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

10. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective

---

[3] *Id*. It is clear that the information exposed as a result of the Data Breach was unencrypted. California law, for example, requires companies to notify California residents "whose **unencrypted** personal information was, or is reasonably believed to have been, acquired by an unauthorized person" due to a "breach of the security of the system[.]" Cal. Civ. Code § 1798.82(a)(1) (emphasis added). Defendant notified the California Attorney General of the Data Breach on Dec. 22, 2021, evidencing that the exposed data was unencrypted. *See also* **Exhibit A**.

security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

11. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (iv) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

12. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

13. Plaintiff David Barocas is a resident and citizen of Phoenix, Arizona. Plaintiff Barocas is acting on his own behalf and on behalf of others similarly situated. Defendant obtained and continues to maintain Plaintiff Barocas' PII and has a legal duty and obligation to protect that PII from unauthorized access and disclosure. Plaintiff Barocas would not have entrusted his PII to Defendant, his former employer, had he known that it would fail to maintain adequate data security. Plaintiff Barocas' PII was compromised and disclosed as a result of the Data Breach.

14. Defendant TTEC is a Colorado corporation with its headquarters in Englewood, Colorado. Defendant is a customer experience and technology company based in Colorado that does business nationwide.[4] Defendant has employed thousands of people, and maintains a workforce of 4,450 employees to operate its business.[5] TTEC is a subsidiary of TTEC Holdings, Inc., a publicly traded company and "one of the largest, global CX (customer experience) technology and services innovators for end-to-end, digital CX solutions[,]" whose "62,000+ employees operate on six continents and bring technology and humanity together to deliver happy customers and differentiated business results."[6]

15. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

16. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed Class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

17. This Court has personal jurisdiction over Defendant because it is authorized to and regularly conducts business in Arizona.

18. Venue is proper in this District under 28 U.S.C. §1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Background

19. Plaintiff and Class Members, as Defendant's employees and customers, were required to provide Defendant with sensitive and confidential information, including their names, date of birth, Healthcare ID number, medical record information, including clinical information

---

[4] *See* https://www.ttec.com/about-us (last visited Feb. 8, 2022).

[5] https://www.dnb.com/business-directory/company-profiles.ttec_services_corporation.558b8d1089a5686b32f5b6ebd0856163.html#:~:text=Ttec%20Services%20Corporation%20has%204%2C450,million%20in%20sales%20(USD) (last visited Feb. 8, 2022).

[6] *See* https://www.ttec.com/about-us (last visited Feb. 8, 2022).

including diagnosis, and/or Social Security numbers, and other PII, which is static, does not change, and can be used to commit countless different types of financial crimes.

20. Plaintiff and Class Members, as current and former employees and as customers of Defendant, relied on the sophistication of Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII.

21. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties.

22. TTEC promises to "take steps to ensure your personal data will be given adequate protection as required by relevant data protection laws and TTEC's internal policies."[7]

23. TTEC states that it:

> complies with the EU-US Privacy Shield and Swiss-US Privacy Shield frameworks as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union ("EU"), the United Kingdom or Switzerland to the United States in reliance on Privacy Shield. TTEC has certified to the U.S. Department of Commerce that it adheres to the Privacy Shield Principles ("Principles") with respect to all such information. If there is any conflict between the Principals and the language in this privacy statement, the Principles will govern.[8]

24. TTEC's commitment to the Privacy Shield Principles includes to "[u]pon notice, take reasonable and appropriate steps to stop and remediate unauthorized processing[.]"[9]

The Data Breach

25. Beginning on or about December 8, 2021, Defendant sent Plaintiff and other current and former employees and customers a *Notice of Data Breach*. Defendant informed the recipients of the notice that:

> We learned that there was unauthorized activity in our network between March 31, 2021 and September 12, 2021. During that time, an unauthorized actor obtained files stored on some of our servers. We completed a careful review of those files and other files on the servers on November 24, 2021 and determined that one or more of the files contained your name and Social Security number.

---

[7] *See* https://www.ttec.com/privacy-policy (last visited Feb. 8, 2022).
[8] *See id*.
[9] *See* https://www.privacyshield.gov/Key-New-Requirements (last visited Feb. 8, 2022).

Other letters stated:

> ***What Information Was Involved***
> Your information involved in this incident included your name and one or more of the following types of information:
> · Date of Birth
> · Healthcare ID Number
> · Clinical Information Including Diagnosis

26. On or about December 8, 2021, Defendant sent data breach notifications to various state Attorneys General, including Vermont, Maine and Montana's Attorney General.[10]

27. Defendant admitted in the letters to the Attorneys General that unauthorized individuals accessed directories that contained PII and were capable of "accessing and acquiring" the PII, including individuals' names, date of birth, Healthcare ID number, medical record information, including clinical information including diagnosis, and/or Social Security numbers.

28. In response to the Data Breach, Defendant claims that "[a]s soon as TTEC learned about the cyber security incident we immediately began an investigation, and cyber security firms that have assisted other organizations with similar matters were engaged. We also notified law enforcement and have been supporting their investigation." The details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again have not been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected.[11]

29. The unencrypted PII of Plaintiff and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

30. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiff and Class Members, causing

---

[10] *See* https://ago.vermont.gov/blog/2021/12/11/ttec-services-corporation-data-breach-notice-to-consumers/ (last visited Feb. 8, 2022); https://apps.web.maine.gov/online/aeviewer/ME/40/a49c129b-d8d5-4f09-beae-9135d8726541.shtml (with link to "Copy of notice to affected Maine residents: TTEC-ME App & Sample.pdf" last visited Feb. 8, 2022); https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-133.pdf (last visited Feb. 8, 2022).

[11] *See id.*

the exposure of PII for many current and former employees, such as encrypting the information or deleting it when it is no longer needed.

31. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[12]

32. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office

[12] *See How to Protect Your Networks from RANSOMWARE*, at 3, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Feb. 8, 2022).

Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[13]

33. To prevent and detect cyber-attacks Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures, which direct organizations to:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….
- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (*e.g.*, contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (*e.g.*, .com instead of .net) …..
- **Open email attachments with caution**. Be wary of opening email attachments, even

[13] *See id*. at 3-4.

from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….
- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[14]

34. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

[14] *See Security Tip (ST19-001) Protecting Against Ransomware* (original release date Apr. 11, 2019), https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Feb. 8, 2022).

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[15]

35. Given that Defendant was storing the PII of its current and former employees and customers, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

36. The occurrence of the Data Breach indicates that Defendant failed to implement adequately one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of an undisclosed amount of current and former employees, including Plaintiff and Class Members.

Defendant Acquires, Collects, and Stores the PII of Plaintiff and Class Members.

37. Defendant has historically acquired, collected, and stored the PII of Plaintiff and

[15] *See Human-operated ransomware attacks: A preventable disaster* (Mar 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Feb. 8, 2022).

Class Members.

38. As a condition of maintaining employment with Defendant, Defendant requires that its employees entrust it with highly confidential PII. Defendant also collects information about employees and customers who use its services, website and business tools. According to Defendant's privacy policy, the information it collects may include:

> … personal data from you, such as your name, postal address, telephone number, e-mail address, credit card number or other payment account number … personal identity numbers, financial account information, racial or ethnic origin, political opinions, religious, philosophical or other similar beliefs, membership of a trade union or profession or trade association, physical or mental health, biometric or genetic data, sexual life, or criminal record (including information about suspected criminal activities). Sensitive personal data may be collected and used in the context of your employment application and relationship with TTEC, to provide you with services you request, or to perform analysis that we may use to improve our website or services and may be shared with our service providers for these purposes. …[16]

39. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

40. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

41. In the ordinary course of doing business with Defendant, customers are required to provide Defendant with PII, such as, but not limited to, payment information. Defendant collects this payment information when it sells products and services. The payment information likely includes financial account numbers, expiration dates, and CVC security codes to process payment cards. Further, in the ordinary course of business Defendant collects and stores PII from prospective, current, and former employees including full name, address, date of birth, Social Security number, and other identifying information as described in paragraph 36.

---

[16] *See* https://www.ttec.com/privacy-policy (last visited Feb. 8, 2022).

Securing PII and Preventing Breaches

42. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data, especially data from former employees.

43. Defendant's policies on its website include promises and legal obligations to maintain and protect PII, demonstrating an understanding of the importance of securing PII. For example, Defendant's Privacy Statement provides in part that it "take[s] reasonable steps to maintain the security of personal data collected via TTEC's websites."[17]

44. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

45. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

46. Defendant does not claim that it abides by the Payment Card Industry Data Security Standard ("PCI DSS"), which is a set of standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. PCI DSS compliance is a requirement for all businesses that store, process, or transmit payment card data.

47. The PCI DSS defines measures for ensuring data protection and consistent security processes and procedures around online financial transactions. Businesses that fail to maintain PCI DSS compliance are subject to steep fines and penalties.

48. As formulated by the PCI Security Standards Council, the mandates of PCI DSS compliance include, in part: Developing and maintaining a security policy that covers all aspects of the business, installing firewalls to protect data, and encrypting payment data that is transmitted over public networks using anti-virus software and updating it regularly.

Value of Personally Identifiable Information

49. The Federal Trade Commission ("FTC") defines identity theft as "a fraud

[17] *See* https://www.ttec.com/privacy-policy (last visited Feb. 8, 2022).

committed or attempted using the identifying information of another person without authority."[18] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[19]

50. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, Personal Information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[20] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[21] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[22]

51. Social Security numbers, for example, are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[23]

---

[18] 17 C.F.R. § 248.201 (2013).

[19] *Id*.

[20] *Your personal data is for sale on the dark web. Here's how much it costs,* DIGITAL TRENDS, Oct. 16, 2019, https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Feb. 8, 2022).

[21] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN, Dec. 6, 2017, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Feb. 8, 2022).

[22] *In the Dark*, VPNOVERVIEW, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Feb. 8, 2022).

[23] Social Security Administration, *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Feb. 8, 2022).

52. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

53. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[24]

54. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, name, date of birth, information about a clinical evaluation or diagnosis, or even a Healthcare ID number.

55. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[25]

56. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

57. The fraudulent activity resulting from the Data Breach may not come to light for years.

58. There may be a time lag between when harm occurs versus when it is discovered,

---

[24] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Feb. 8, 2022).

[25] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Feb. 8, 2022).

and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[26]

59. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers and dates of birth, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

60. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

61. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's servers, amounting to potentially thousands of individuals' detailed, PII and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

62. In the breach notification letter, Defendant made an offer of 12 months of identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, medical and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

63. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

64. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class

---

[26] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last visited Feb. 8, 2022).

Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Plaintiff David Barocas's Experience

65. Plaintiff Barocas was required to provide his PII to Defendant in connection with his employment, which started in or about September of 2017 and ended in or about October 2017. Plaintiff Barocas was also employed with Defendant in February of 2018.

66. On or about December 8, 2021, Plaintiff Barocas received notice from Defendant that his PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Barocas' PII, including name and Social Security number, was compromised as a result of the Data Breach.

67. Plaintiff Barocas made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; researching and signing up for credit monitoring and identity theft protection services offered by Defendant; and contacting creditors and credit bureaus. Plaintiff Barocas has spent at least five hours dealing with the Data Breach, valuable time Plaintiff Barocas otherwise would have spent on other activities, including but not limited to work and/or recreation.

68. As a result of the Data Breach, Plaintiff Barocas has suffered emotional distress due to the release of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff Barocas is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

69. Plaintiff Barocas suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of his PII, a form of property that Defendant obtained from Plaintiff Barocas; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

70. As a result of the Data Breach, Plaintiff Barocas anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data

Breach. As a result of the Data Breach, Plaintiff Barocas is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS ALLEGATIONS

71. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, for the following class:

> **All individuals residing in the United States whose PII was compromised in the data breach first announced by Defendant on or about December 8, 2021 (the "Nationwide Class").**

72. The Arizona Subclass is defined as follows:

> **All individuals residing in Arizona whose PII was compromised in the data breach first announced by Defendant on or about December 8, 2021 (the "Arizona Subclass").**

The Nationwide Class and Arizona Subclass are collectively referred to herein as the "Class."

73. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

74. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

75. Numerosity, Fed R. Civ. P. 23(a)(1): The Class is so numerous that joinder of all members is impracticable. The Class is apparently identifiable within Defendant's records.

76. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant had a duty not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had a duty not to use the PII of Plaintiff and Class Members for

non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

77. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because he had his PII compromised as a result of the Data Breach due to Defendant's misfeasance.

78. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members

uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

79. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages he has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

80. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against a large corporation, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

81. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged for the following reasons: (i) Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; (ii) the costs of individual suits could unreasonably consume the amounts that would be recovered; (iii) proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and (iv) individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

82. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

83. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

84. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

85. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

86. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;
b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;
c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;
e. Whether Defendant breached the implied contract;
f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members; and,

i. Whether Class Members are entitled to actual damages, statutory damages, nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class)

87. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 86.

88. As a condition of their employment with Defendant or by purchasing goods or services from Defendant, Defendant's current and former employees and customers were obligated to provide Defendant with PII, among other sensitive PII, their names, dates of birth, and Social Security numbers.

89. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

90. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

91. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

92. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII of Plaintiff and the Class in Defendant's

possession was adequately secured and protected.

93. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former employees' PII that Defendant was no longer required to retain pursuant to regulations.

94. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiff and the Class.

95. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of employment with the company or making purchases from Defendant.

96. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

97. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

98. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting or redacting PII stored on Defendant's systems.

99. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions to not comply with industry standards for the safekeeping of the PII of Plaintiff and the Class, including basic encryption techniques freely available to Defendant.

100. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

101. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

102. Defendant had and continues to have a duty to adequately disclose that the PII of

Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

103. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Class.

104. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

105. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Class during the time the PII was within Defendant's possession or control.

106. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

107. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiff and the Class in the face of increased risk of theft.

108. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of its current and former employees' PII.

109. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

110. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

111. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and the present harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding

such PII by adopting, implementing, and maintaining appropriate security measures.

112. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

113. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

114. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

115. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

116. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

117. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate

measures to protect the PII of Plaintiff and the Class; and (viii) costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

118. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

119. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

120. Plaintiff and Class Members are therefore entitled to damages, including restitution and unjust enrichment, declaratory and injunctive relief, and attorney fees, costs, and expenses.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Nationwide Class)

121. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 86.

122. Defendant required Plaintiff and the Class to provide their PII, including names, dates of birth, Social Security numbers and other PII, as a condition of their employment or purchases.

123. As a condition of their employment with or purchases from Defendant, Plaintiff and the Class provided their PII. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

124. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

125. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their PII, and by failing to provide timely and accurate notice to them that their PII was compromised as a result of the Data Breach.

126. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer): ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

COUNT III
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Nationwide Class)

127. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 86.

128. Plaintiff and the Class had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

129. Defendant owed a duty to its current and former customers and employees, including Plaintiff and the Class, to keep their PII confidential.

130. Defendant failed to protect and released to unknown and unauthorized third parties the PII of Plaintiff and the Class.

131. Defendant allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiff and the Class, by way of Defendant's failure to protect the PII.

132. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and the Class is highly offensive to a reasonable person.

133. The intrusion was into a place or thing which was private and is entitled to be private. Plaintiff and the Class disclosed their PII to Defendant as part of the current and former employees' employment with Defendant and/or during a consumer transaction with Defendant,

but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

134. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

135. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

136. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Class.

137. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiff and the Class was disclosed to third parties without authorization, causing Plaintiff and the Class to suffer damages.

138. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Class have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

COUNT IV
BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Nationwide Class)

139. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 86.

140. At all times during Plaintiff's and the Class's interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and the Class's PII that Plaintiff and the Class provided to Defendant.

141. As alleged herein and above, Defendant's relationship with Plaintiff and the Class was governed by terms and expectations that Plaintiff's and the Class's PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

142. Plaintiff and the Class provided their PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized third parties.

143. Plaintiff and the Class also provided Plaintiff's and the Class's PII to Defendant with the explicit and implicit understanding that Defendant would take precautions to protect that PII from unauthorized disclosure.

144. Defendant voluntarily received in confidence Plaintiff's and the Class's PII with the understanding that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

145. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiff's and the Class's PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and the Class's confidence, and without their express permission.

146. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and the Class have suffered damages.

147. But for Defendant's disclosure of Plaintiff's and the Class's PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and the Class's PII as well as the resulting damages.

148. The injury and harm Plaintiff and the Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and the Class's PII. Defendant knew or should have known its methods of accepting and securing Plaintiff's and the Class's PII was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and the Class's PII.

149. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Class, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the

compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of current and former customers and employees; and (viii) present and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

150. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT V
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Nationwide Class)

151. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 86.

152. Defendant benefited from receiving Plaintiff's and Class Members' PII by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

153. Defendant also understood and appreciated that Plaintiff's and Class Members' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that PII.

154. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of their employment and by purchasing goods from Defendant, and in connection thereto, by providing their PII to Defendant with the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures. Specifically,

they were required to provide Defendant with their PII. In exchange, Plaintiff and Class members should have received adequate protection and data security for such PII held by Defendant.

155. Defendant knew Plaintiff and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

156. Defendant failed to provide reasonable security, safeguards, and protections to the PII of Plaintiff and Class Members.

157. Under the principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiff and Class members, because Defendant failed to implement appropriate data management and security measures mandated by industry standards.

158. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

159. Defendant's enrichment at the expense of Plaintiff and Class Members is and was unjust.

160. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

COUNT VI
VIOLATION OF THE ARIZONA CONSUMER FRAUD ACT
A.R.S. REV. STAT. § 44-1522 *et seq.*
(On Behalf of Plaintiff and the Arizona Subclass)

161. Plaintiff and the Arizona Class re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 86.

162. Plaintiff and the Arizona Class Members were employed by Defendant and were engaged in transactions and conduct to procure merchandise or services in connection with Defendant.

163. Defendant engaged in transactions and conduct to procure merchandise or services on behalf of Plaintiff and Class Members as defined by Arizona Revised Statues ("A.R.S.") § 44-1521(5).

164. Defendant engaged in trade and commerce through its acts and omissions and its course of business, including marketing, offering to sell, and selling sporting goods throughout the United States.

165. Defendant violated A.R.S. section 44-1522, *et seq.* by engaging in deceptive, unfair, and unlawful trade acts or practices that were committed in Arizona, while conducting trade or commerce in Arizona. Defendant's violations include, but are not limited to:

a. A failure to safeguard customer PII through data security practices and computer systems;

b. A failure to disclose that their computer systems and data security practices were inadequate to protect PII;

c. A failure to notify Plaintiff and Class Members in a timely manner of the data breach;

d. A failure to stop accepting and storing PII after the Defendant knew or should have known that the vulnerabilities were exploited in a data breach;

e. A failure to remediate the vulnerabilities that allowed the Data Breach to happen.

f. A misrepresentation and/or omission regarding its commitment to give adequate protection to PII; and

g. A failure to take reasonable and appropriate steps to stop and remediate unauthorized processing.

166. These unfair acts and practices violate the duties imposed by, but not limited to, the FTCA and A.R.S. section 44-1522(A).

167. As a direct result of these violations, Plaintiff and Class Members suffered damages. These damages include, but are not limited to:

a. Lost time spent constantly checking their credit for unauthorized activity, which is necessary to do to protect themselves from the consequences of having their PII available on the dark web because of the Data Breach; and

b. Other economic damage that may not be detected for years to come.

168. Plaintiff and Class Members are entitled to damages as well as injunctive relief because of Defendant's knowing violation of Arizona Consumer Fraud Act. These include, but are not limited to, ordering that Defendant:

a. Utilize third-party security professionals to regularly test for security vulnerabilities;

b. Utilize third-party security professionals and internal personnel to perform automated security monitoring;

c. Train security personnel on how to audit and test any new or modified security protocols;

d. Protect data by securing it separately from other portions of the network;

e. Delete PII that is no longer necessary to provide services;

f. Conduct regular database security checks;

g. Provide regular training to internal security personnel on how to identify and contain a breach and what to do when a breach occurs; and

h. Educate class members about the threats they face now that their PII is available to unauthorized third parties and steps that patients can take to protect themselves.

169. Plaintiff brings this action on behalf of himself and Arizona Class Members for the relief requested above. This action will also protect the public from Defendant's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and unlawful practices.

170. The deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. The acts caused substantial injury to Plaintiff and Arizona Class Members that they could not reasonably avoid and the injuries suffered outweigh any benefit to patient-consumers or to competition.

171. Defendant knew or should have known that the computer systems and data security protocols were inadequate to store sensitive PII, which put the data at an increased risk of theft or breach.

172. Defendant's unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless.

173. Plaintiff and Arizona Class Members seek relief under the Arizona Consumer Fraud Act (A.R.S. § 44-1522(A)). The relief includes, but is not limited to, damages, restitution, injunction relief, and/or attorney fees and costs, and any other just and proper relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class, as defined herein, and appointing Plaintiff and his Counsel to represent each such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as

necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Dated: February 8, 2022

Respectfully Submitted,

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP

By: */s/ Betsy C. Manifold*
BETSY C. MANIFOLD

BETSY C. MANIFOLD (*pro hac vice* forthcoming)
RACHELE R. BYRD (*pro hac vice* forthcoming)
OANA CONSTANTIN (*pro hac vice* forthcoming)
750 B Street, Suite 1820
San Diego, CA 92101

Telephone: (619) 239-4599
Facsimile: (619) 234-4599
manifold@whafh.com
byrd@whafh.com
constantin@whafh.com

M. ANDERSON BERRY (*pro hac vice* forthcoming)
GREGORY HAROUTUNIAN (*pro hac vice* forthcoming)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Facsimile: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com

Attorneys for Plaintiff and the Proposed Class

28009v6